
Inhaltsverzeichnis

1	Einführung	1
1.1	Motivation und Problemstellung	1
1.2	Zielsetzung der Methodik zur Systemanalyse	3
1.3	Gliederung der Arbeit	4
2	Charakteristika mechatronischer, verteilter, sicherheitsrelevanter Kraftfahrzeugsysteme	6
2.1	Eigenschaften mechatronischer Systeme	6
2.2	Eigenschaften sicherheitsrelevanter Systeme	7
2.3	Eigenschaften verteilter Systeme	9
2.4	Beispiele und Konzeptionen für heutige und zukünftige mechatronische, verteilte, sicherheitsrelevante Kraftfahrzeugsysteme	9
3	Anforderungen an eine modellbasierte, ganzheitliche Systemanalyse	16
3.1	Anforderungen an die Analysemethode	16
3.2	Anforderungen an das Modellierungskonzept	17
4	Vergleichende Analyse und Bewertung bekannter Methoden im Themenkomplex der Systemanalyse	19
4.1	Methoden der System- und Sicherheitsanalyse	19
4.1.1	HAZOP-Verfahren	21
4.1.2	Fehlermöglichkeits- und Einflussanalyse	22
4.1.3	Fehlerbaum-Analyse	25
4.1.4	ETA-Verfahren	27
4.1.5	Markov-Analyse	28
4.1.6	Formale Methoden	30
4.1.7	Zusammenfassung der diskutierten Methoden	32

4.2	Modellierungskonzepte	33
4.2.1	Graphen als Modellelemente eines zustandsorientierten Konzepts	34
4.2.2	Zustandsautomaten	35
4.2.3	Petri-Netze als Elemente eines zustandsorientierten Konzepts	36
4.2.4	CARTRONIC als objektorientierte Modellierungstechnik	37
4.2.5	Qualitative Modellierung in einem prozessorientierten Konzept	38
4.2.6	Quantitative Modellierung in einem prozessorientierten Konzept	39
4.2.7	Hybride Modellierung	40
4.2.8	Zusammenfassung	41
4.3	Methoden zur Automatisierung von System- und Sicherheitsanalysen	43
5	Konzept der ganzheitlichen, dynamischen Systemanalyse	46
5.1	Methodik der ganzheitlichen, dynamischen Analyse	46
5.2	Einbettung in einen Entwicklungsprozess	50
6	Quantitative hybride Gesamtsystemmodellierung	52
6.1	Klassifizierung von Systemen und Systemkomponenten	52
6.2	Modellierung unter funktionalen Aspekten	55
6.2.1	Modell des zu untersuchenden Kraftfahrzeugsystems	55
6.2.2	Fahrzeugmodell	55
6.2.3	Fahrermodell	56
6.2.4	Umweltmodellierung	57
6.3	Modellierung unter strukturellen Aspekten	58
6.3.1	Erweiterung des Kraftfahrzeugsystemmodells	59
6.4	Modellierung unter Sicherheitsaspekten	60
6.4.1	Fehlermodelle	61
6.4.2	Erweiterung des Kraftfahrzeugsystemmodells	63
6.4.3	Fehlerinjektion	64
6.4.4	Objektiv-quantifizierbare Bewertungsfunktion	64

7	Identifikation signifikanter Fehler	66
7.1	Algorithmen zur globalen Suche	66
7.1.1	Monte Carlo Methode	66
7.1.2	Simulated Annealing	66
7.1.3	Genetische Algorithmen	67
7.2	Evolutionäre Programme	67
7.2.1	Aufbau und Funktionsweise	68
7.2.2	Selektionsverfahren	69
7.2.3	Evolutionäre Operatoren	70
7.2.4	Erweiterungen zum Umgang mit Nebenbedingungen	72
7.3	Identifikation von Einzelfehlern	75
7.4	Erweiterungen	76
7.4.1	Identifikation von Fehlerkombinationen	76
7.4.2	Identifikation von Fehlersequenzen	77
7.4.3	Verknüpfung mit Fehlerauftrittswahrscheinlichkeiten	78
7.5	Visualisierung	79
7.6	Parallele und skalierbare Anwendung	82
7.7	„What happened“-Analyse	85
7.8	Iterative Durchführung	86
7.9	Anmerkungen	87
8	Anwendung am Beispiel eines steer-by-wire Systems	88
8.1	Systemarchitektur der Beispielanwendung	88
8.2	Gesamtsystemmodellierung	90
8.2.1	Überblick zur Simulationsumgebung	90
8.2.2	Modellierung unter funktionalen Aspekten	92
8.2.3	Modellierung der Systemumwelt	95
8.2.4	Modellierung unter strukturellen Aspekten	96
8.2.5	Modellierung unter Sicherheitsaspekten	97
8.3	Identifikation signifikanter Fehlerszenarien	102
8.3.1	Objektiv-quantifizierbare Bewertungsfunktion	103

8.3.2	Parametrierung, Fehlerinjektion und Ergebnisse	105
8.3.3	What happened - Analyse	109
8.3.4	Iterative Anwendung	110
8.3.5	Reproduzierbarkeit des Identifikationsergebnisses	111
8.3.6	Einfluss der Parameter des evolutionären Algorithmus auf das Identifikationsergebnis	112
9	Zusammenfassung und Ausblick	115
9.1	Zusammenfassung	115
9.2	Bewertung und Erkenntnisse	116
9.3	Ausblick	118
A	Ein redundantes, synchronisiertes TTCAN-Kommunikationsnetz	121
A.1	Einführung in das TTCAN-Kommunikationsprotokoll	121
A.2	Synchronisationsalgorithmus	123
A.3	Analyse des Fehlerverhaltens	126
A.3.1	Fehler, die das zeitliche Verhalten beeinflussen	127
A.3.2	Fehler, die die Nachrichteninhalte beeinflussen	133
	Literaturverzeichnis	144